

- 2 -

In the claims:

All claims presented for examination are listed below.

~~Claim 1~~ [[:]] : (Currently amended) ~~A method and~~ An apparatus to secure online transactions on the Internet comprising:

- a smart card transmitting an identification sequence to a PC in the form of a modulated signal[[:]] ;
 - a card reader plugged into the microphone input of the PC sound card[[:]] ; and
 - a PC applet demodulating the identification sequence[[:]]
- and characterized by the absence of processing means within the card reader.

~~Claim 2~~ [[:]] : (Currently amended) ~~A method as in~~ The apparatus of claim 1, wherein the identification sequence comprises at least a unique card number and a random number valid only once.

~~Claim 3~~ [[:]] : (Currently amended) ~~A method as in~~ The apparatus of claim 2, wherein the random number is a session key (Ki) which is not transmitted to the authentication server.

~~Claim 4~~ [[:]] : (Currently amended) ~~A method as in~~ The apparatus of claim 3, wherein the session key (Ki) is a function of the previous one (Ki-1) emitted by the card, wherein such as: $K_i = G(K_{i-1})$ [[:]] and G is a one-way function also known by the authentication server.

~~Claim 5~~ [[:]] : (Currently amended) ~~A method as in~~ The apparatus of claim 4, wherein the session key (Ki) is used by the PC applet to generate a message authentication code (MAC) of the password entered by the user; said first MAC is transmitted to the authentication server along with the card number.

- 3 -

~~Claim 6~~[[:]] . (Currently amended) The apparatus of A method as in claim 5, wherein the authentication server generates a second MAC of the password stored in the authentication server database, using a session key deduced from the previous one (Ki-1) also stored in the database.

~~Claim 7~~[[:]] . (Currently amended) The apparatus of A method as in claim 6, wherein the authentication is valid only if said first and second MAC are identical; if this is the case, the authentication server replaces (Ki- 1) by (Ki) in the database and (Ki) cannot be reused.

~~Claim 8~~[[:]] . (Currently amended) The [[An]] apparatus as in claim 1, wherein the smart card is powered by the voltage provided by the microphone input of the PC sound card.

~~Claim 9~~[[:]] . (Currently amended) The [[An]] apparatus as in claim 8, wherein the smart card transmits the modulated signal when the switch of the card reader is pressed by the user.

~~Claim 10~~[[:]] . (Currently amended) The [[An]] apparatus as in claim 9, wherein the smart card transmits the modulated signal to the microphone input through the ISO contact C6.

~~Claim 11~~[[:]] . (Currently amended) The [[An]] apparatus as in claim 10, wherein the smart card transmits the modulated signal when the ISO contact C2 is pulled down.

~~Claim 12~~[[:]] . (Currently amended) The [[An]] apparatus as in claim 11, wherein the smart card is powered through the ISO contacts C4 and C8.

- 4 -

Claim 13[:]. (Currently amended) The [[An]] apparatus as in claim 1, wherein the card reader further comprises a battery cell powering the card; said reader is alternatively plugged into the line input of the PC sound card.

~~Claim 14[:]~~ (Canceled)

~~Claim 15[:]~~ (Currently amended) The [[An]] apparatus as in claim 1, wherein the card reader is further integrated into the PC unit or display.

16. (New) A method for securing online transactions on the Internet comprising:

- (a) providing a smart card for transmitting an identification sequence by a smart card to a PC in the form of a modulated signal;
- (b) plugging a card reader into the microphone input of the PC sound card the card reader devoid of processing means; and
- (c) demodulating the identification sequence by a PC applet.

17. (New) The method of claim 1, wherein the identification sequence in step (a) comprises at least a unique card number and a random number valid only once.

18. (New) The method of claim 17, wherein the random number is a session key (K_i) which is not transmitted to the authentication server.

19. (New) The method of claim 18, wherein the session key (K_i) is a function of the previous one (K_{i-1}) emitted by the card, wherein $K_i = G(K_{i-1})$ and G is a one-way function also known by the authentication server.

20. (New) The method of claim 18, wherein the session key (K_i) is used by the PC applet to generate a message authentication code (MAC) of the password entered by the user; said first MAC is transmitted to the authentication server along with the card number.

- 5 -

21. (New) The method of claim 20, wherein the authentication server generates a second MAC of the password stored in the authentication server database, using a session key deduced from the previous one (Ki-1) also stored in the database.

22. (New) The method of claim 21, wherein the authentication is valid only if said first and second MAC are identical; if this is the case, the authentication server replaces (Ki-1) by (Ki) in the database and (Ki) cannot be reused.